



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

DANIYAL MARGHOOB

DESIGN AND IMPLEMENTATION OF SECURE COMMUNICA-
TION OF JOT AUTOMATION MACHINES TO CLOUD SERVICES

Master of Science Thesis

Examiner: Prof. Eric Coatanea
Examiner and topic approved by the
Faculty Council of the Faculty of
Engineering Sciences
on 9th September 2017

ABSTRACT

Daniyal Marghoob: TUT Thesis

Tampere University of technology

Master of Science Thesis, 46 pages,

September 2017

Master's Degree Programme in Automation Engineering

Major: Factory Automation and Industrial Informatics

Examiner: Professor Eric Coatanea

Keywords: IoT, IIoT, JOT Automation, Cloud Services, AWS, MQTT, HTTP, ZigBee, WiFi, Communication, SME's, MEC, TLS, SSL

In past few years, almost every industry puts lot of effort in introducing Internet of Things to expand production volume while maintaining low cost and increase the energy efficiency. Several different techniques have been introduced to achieve the goal of real-time and bi-directional communication. However, the problem of scalability and security in the domain of IoT is still to be solved. Absence or maturity level of these two features hinders this technology from its way to factory floor. Moreover, there is no generic solution on a global scale of IoT security and scalability.

The main focus of this thesis is to provide big picture of Industrial Internet of Things to readers with different possibilities of IIoT implementation for small and medium sized enterprises. In addition to this, thesis also focuses on working, benefits, disadvantages and comparison between different old and emerging technologies with several use cases, options and practical implementation of IIoT concept on JOT Automation products to build real time, modular, bi-directional, scalable and secure system.

The proposed approach is based on maturity level of IoT stack protocols and cloud services. Architecture of system is designed in such a way that it can be integrated to current ERP solution. The results and final application reflects the effectiveness of approach.

PREFACE

Motivation of this thesis research work is to provide new domain low-cost and efficient solution for organizations to increase the economic growth of country and open new business areas for SME's to create new job opportunities.

First and foremost, I am thankful to Al-Mighty for giving me strength and ability to learn and understand the diverse technologies as well as helping me to complete this research on time. It has been a great experience for being a student at TUT and employee at JOT Automation at the same time.

This research was not possible without help, support, effort and mentoring of Antti Kaihua (R&D Manager, JOT Automation) and Rami Rahikkala (SW Team Lead, JOT Automation). I would also like to thank Professor Eric Coatanea, for his kindness, support and supervision on this work at university and giving a valuable feedback for continuously improvement.

I am also very grateful to my friends, especially Ammar Bukhari, Adnan Mushtaq, Aitzaz Hassan, Hafiz Ammar, Mansur Ahmed and Qasim Mehdi for keeping me motivated and helping me out in hour of need.

People I can't pay regard for their love, kindness and affection in words are my parents, who prayed for me.

Tampere, 29.09.2017

Daniyal Marghoob

CONTENTS

1.	INTRODUCTION	1
2.	THEORETICAL BACKGROUND AND RESEARCH METHODOLOGIES	2
2.1	Industrial Revolution:.....	2
2.2	Current IIoT Implementations.....	3
3.	RESEARCH METHODOLOGIES AND MATERIAL	8
3.1	IoT Hardwares	8
3.2	IoT Networks.....	11
3.2.1	IEEE 802.15.4 and ZigBee	12
3.2.2	IEEE 802.15.1 Bluetooth and Bluetooth LE.....	14
3.2.3	IEEE 802.11 WLAN/Wi-Fi	16
3.2.4	Near Field Communication (NFC)	19
3.2.5	Z-Wave.....	20
3.2.6	Comparison between IoT network layer protocols	22
3.3	IoT Cloud Platforms:.....	22
3.3.1	Comparison between mature IoT cloud Platforms	24
3.4	IoT Application Layer:.....	25
3.4.1	Message Queue Telemetry Transport (MQTT)	26
3.4.2	Constrained Application Protocol (CoAP)	27
3.4.3	Extensible Messaging and Presence Protocol (XMPP):	29
3.4.4	Hyper Text Transfer Protocol (HTTP).....	30
3.4.5	Comparison between IoT network layer protocols	32
4.	PRACTICAL IMPLEMENTATION.....	33
4.1	PTC Incorporation Framework	33
4.1.1	Working and benefit of Smart Connected Products.....	34
4.2	Proposed Architecture	35
4.3	Selection criteria.....	35
4.3.1	Setup.....	36
4.4	Different Options and Use-cases.....	38
4.5	Advantages	41
5.	CONCLUSIONS.....	42
6.	REFERENCES.....	43

LIST OF FIGURES

<i>Figure 2.1: Industrial Revolution</i>	<i>2</i>
<i>Figure 3.1: General four layer IoT application architecture</i>	<i>12</i>
<i>Figure 3.2: ZigBee Network Topologies</i>	<i>13</i>
<i>Figure 3.3: Connectivity of devices with fixed Bluetooth LE gateway</i>	<i>15</i>
<i>Figure 3.4: WLAN Infrastructure</i>	<i>17</i>
<i>Figure 3.5: Connection establishment between Station (client) and Access Point.....</i>	<i>18</i>
<i>Figure 3.6: NFC: Different modes of operation</i>	<i>19</i>
<i>Figure 3.7: Z-Wave wireless network architecture.....</i>	<i>20</i>
<i>Figure 3.8: Z-Wave protocol four layer OSI model.....</i>	<i>21</i>
<i>Figure 3.9: MQTT protocol architecture.....</i>	<i>26</i>
<i>Figure 3.10: CoAP Public Key Sharing.....</i>	<i>28</i>
<i>Figure 3.11: CoAP Message Format.....</i>	<i>29</i>
<i>Figure 3.12: A simple XMPP architecture with two clients</i>	<i>29</i>
<i>Figure 3.13: HTTP client/server communication</i>	<i>31</i>
<i>Figure 4.1: IIoT PTC Inc. Framework.....</i>	<i>33</i>
<i>Figure 4.2: JOT Automation IIoT System of Systems</i>	<i>34</i>
<i>Figure 4.3: IIoT data flow and working on factory floor</i>	<i>34</i>
<i>Figure 4.4: Proposed architectural solution</i>	<i>35</i>
<i>Figure 4.5: Hardware setup.....</i>	<i>37</i>
<i>Figure 4.6: IIoT Option 1</i>	<i>38</i>
<i>Figure 4.7: Option 2 using ZigBee connectivity to form mesh for data transmission.....</i>	<i>40</i>
<i>Figure 4.8: Star of stars topology for whole system</i>	<i>41</i>

LIST OF TABLES

<i>Table 3.1: Hardware Comparison</i>	<i>10</i>
<i>Table 3.2: WLAN Standards and Bandwidths</i>	<i>16</i>
<i>Table 3.3: Comparison between IoT communcation</i>	<i>22</i>
<i>Table 3.4: Comparison between IoT Cloud Platforms</i>	<i>25</i>
<i>Table 3.5: MQTT vs HTTPS</i>	<i>27</i>
<i>Table 3.6: Comparison between application layer protocols.....</i>	<i>32</i>

LIST OF SYMBOLS AND ABBREVIATIONS

IoT	Internet of Things
IIoT	Industrial Internet of Things
HTML	HyperText Markup Language
TUT	Tampere University of Technology
URL	Uniform Resource Locator
BLE	Bluetooth Low Energy
PAN	Personal Area Network
UHF	Ultra High Frequency
WLAN	Wireless Local Area Network
ESS	External Service Set
NFC	Near Field Communication
P2P	Peer-to-peer
RFID	Radio Frequency Identification
MQTT	Message Queue Telemetry Transport
CoAP	Constrained Application Protocol
XMPP	Extensible Messaging and Presence Protocol
HTTP	HyperText Transfer Protocol
TLS	Transport Layer Security
SASL	Simple Authentication & Security Layer
TCP	Transmission Control Protocol
IP	Internet Protocol
SME	Small Medium Size Enterprise
MEC	Mobile Edge Computing

.

1. INTRODUCTION

World is changing rapidly and so do technology. There are enormous opportunities through which physical objects can be controlled over distances. This introduces area of Internet of Things. IoT not only allow users to interact with internal states of devices but also there interaction with external environments. Industrial IoT or concept of industry 4.0 emerges from IoT, which is to provide control of industrial devices to perform computations and to store and extracts useful data. This data can be used for forecasting the production revenue, control quality of production, predictive maintenance of industrial equipment's and soon.

The IoT was first introduced to industry in September 2003, when it was used to track the record of goods in supply-chain [1]. After that, it gains interests of researchers. Initially, it was a problem to transmit data so that it can be visualized to observe the flow. Later, there came a need to store a data effectively which can be retrieved back. Security of data remains the problem for the very beginning. Un-secure communication of devices introduces ambiguities and allows anyone to enter in system. Researchers put effort to solve this problem by introducing several protocols and security measures to solve this problem but they were unable to provide such a solution which could be adopted by all the industries as a standard.

The concern of industries to adapt any solution as a standard is also fair enough because it is almost impossible for one solution to cover all the requirements. This paper provides detailed discussion of protocols, hardware selection and their comparison with different architectural options which can be adopted by manufacturing with little modifications according to their needs. While doing research, intention of author was quite clear to provide cost effective, easy to implement, optimized and integration solution for SME's.

This thesis is constructed in such a manner, it explains all the aspects of IIoT, which allows SME's to introduce this concept to enhance their production capabilities. Chapter 2 illustrates about previous researches and work done related to this technology, followed by Chapter 3 which explains about all the short and long range technologies, cloud services and communication protocols. Chapter 4 is about the actual implementation of IIoT on JOT Automation M10 box, which is used for quality control. Moreover, this chapter also includes several use-cases, options and selection of IoT hardwares, communication protocols and cloud computational services. Finally, Chapter 5 concludes this paper by providing potential future opportunities and limitations regarding this research work

2. THEORETICAL BACKGROUND AND RE-SEARCH METHODOLOGIES

This chapter briefs about history of industrial revolution with deep insight of current implementations, which are being used to implement the concept of Industrial Internet of Things.

2.1 Industrial Revolution:

During the era of late 1700's till 1840's, mechanization was introduced in industry to speed up the work. This industrial revolution focused on reducing human efforts by bringing mechanical tools in production. In 1870, second industrial revolution came to reduce human efforts further by implementing electrification to factory floors. This is the era which introduced concept of assembly line as well as provide the introduction to automobiles and combustion engines [2].

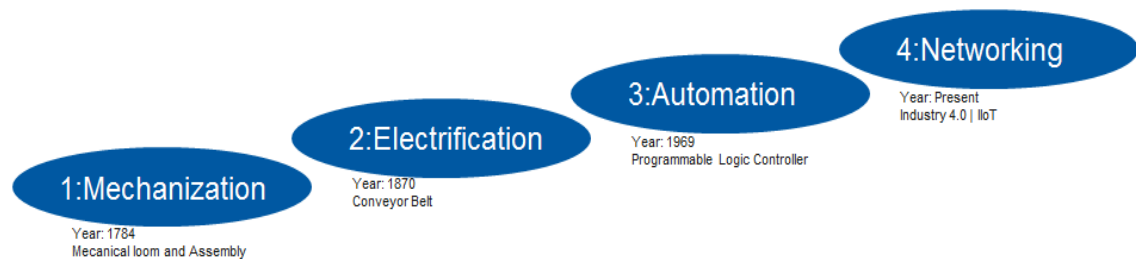


Figure 2.1: Industrial Revolution

During the period after 1870 to late 1900's, there was need to introduce digitization to industrial equipment's, where automation played an important role. By integrating controllers to industrial equipment's, human efforts reduced significantly. Programmable logic controllers (PLC) were also introduced during this era. The automation processes not only decreases the production time but also at the same time, increased the quality of product by taking precise measurements from sensors. After automating the factory floor, there was a need of transmission of meaningful data to executive hierarchy of organization as well as need a mean to communicate machines and systems on factory floors with each other. This need of industry increased the demand of computer networks, data management and software skill [3].

In 2011, German government introduces the new concept of industrial networking as a part of their economic policy and named it as "Industry 4.0". This concept is based on already existing technologies like cyber-physical systems and Internet of Things (IoT).

These technologies not only allow data and information exchange between humans but also between humans and machines with additional feature of machine to machine (M2M) communication. Industry 4.0 or Industrial Internet of Things leads to establishment of continuous, real time and live data communication. This sort of technology not only allows the retailers to keep information regarding the production but also provide information to consumers regarding the production of their orders. Small and medium sized (SME) organizations are the one who are expecting to gain most out this industrial revolution. [4]

The progress of Industry 4.0 or IIoT can evaluated by following three points,

1. Managing information by planning production systems, this leads to digitization in production.
2. Acquire useful information from production equipment's.
3. A way to link manufacturing sites with supply chain.

The main purpose of IIoT is to collect and analyze information from the human surroundings, to design a well-regulated economy and to improve the services. One cannot restricts Industry 4.0 or IIoT revolution to robotics, automation or factory floor because evolution of this technology will effect whole business processes from ordering materials to dispatching products to end customers. Introduction of this technology in products will be of added value. In addition, IIoT provides the facility to monitor the production equipment's to control production quality and energy management. The transmission of information, through connectivity of factory floor or production unit devices to executive management of organization allows forecasting, that will eventually plays a vital role in decision making and strategy planning.

Integration of devices with cloud computing for storage of data is also a part of IIoT. It provides with different options and possibilities to optimize the equipment in production as well as helps in predictive maintenance [5].

2.2 Current IIoT Implementations

World is changing rapidly and so are manufacturing industries. Previously, on factory floor, data was gathered manually through employee on some papers. That was inefficient because most of the time half of data losses due to no proper method or technique to store it. With the passage of time, sensors became inexpensive and opportunities of collecting real time data increases. With the increase in data, there was need to gather and collect data from separated traditional systems. That was the point when IoT was introduced in the industry. IIoT (industrial Internet of Things) also named as Industry 4.0 (by some researchers, helps in transition of raw data from factory floor to executive

level business insights. Based on that data, management can perform analysis and make strategies. These strategies or use cases are also known as IIoT strategies.

Characteristics of IoT data gathered from factory floor are divided into four categories.

1. **Streaming:** Real time high velocity and continuous data logging of machines (messages and alerts).
2. **High Volume:** Require data management and high performance data manipulation to make data useful.
3. **Semi-Structured:** Not properly structured and modeled data, require additional effort for parsing and converting into structural schematic form, which is easy to be analyzed.
4. **Non-Standard:** Requires transformation to use it. [6]

Most of the industry use IoT for collecting data from systems that involves Asset Tracking (RFID and GPS), control room (HVAC), predictive maintenance (machine learning), autonomous robots (robotic operating system), augmented reality and additive manufacturing. It helps in cost savings, revenue generation, customer loyalty, ownership and service.

Data analysis is categorized in four for data coming from factory floor.

1. **Replacing traditional data into Collection:** Connect and integrate IoT devices with current system for data collection and storage for both real-time and legacy data.
2. **Descriptive Analysis:** Based on data stored in database and continuous stream of run time data, this analysis runs and results in the detail overview of factory floor.
3. **Predictive Analysis:** Based on all the data gathered from system, forecast the situation by using machine learning techniques and tools.
4. **Prescriptive Analysis:** Based on the data gathered from system, find out the probability of fault and auto corrects it with minimum human effort. [6]

In order to make business profitable and smart, manufacturers are implementing IoT. Some of the strategically use cases are as follow.

- **Swift Costing:** It is considered that manufacturing functions and utilities are the part of product management group. So, it must be rapid and quick in order to calculate the turnaround of factors that depicts win or lose situation of enter-

prise. IIoT helps in the prediction of tendering and provide valid and quick feedback.

- ***Non-Conformance Report (NCR) Analytics:*** It includes the faults in products, processor procedures, when they are not meeting any set of standards. IIoT helps in find a way to support and forecast the non-conformance. [7]
- ***Plant Efficiency Control:*** Operations are the core of any manufacturing industry. It helps upper level management to create a strategic plans and tactics on daily basis. IIoT allows the management to analyze current scenario and plan a strategy based on data collection from factory floor in order to compete in market. [6]
- ***Improvement in Factory Floor:*** All manufacturers always want to have inexpensive sensors and systems on factory floor. In order to maintain that system, continuous flow of data is required, so that after being analyzed, management can depict the malfunctioning of part beforehand and prevent system from going down. IIoT solutions help to improve the overall efficiency of system by minimizing the chances of failure.
- ***Supply Chain:*** With the help of IoT, all the vendors connected with manufactures are being informed about the current scenario and potential requirements. IIoT enabled plant to connect with suppliers and help in maintaining inventory, location tracing and material flow by collecting delivery information into ERP and product lifecycle management.
- ***Safety:*** IIoT allows management to analyze about the Key Performance Indicators for health, safety and environment. Sensor in the machines and IoT bands on workers on factory floor provide data, which enables management to monitor and react to eliminate the root cause of any damage. [7]

It is estimated that by 2030, the economic value of IIoT will reach to 15 trillion USD. Frank Gillet, vice president of Forrester states that companies are serious to adopt IIoT as, they want to save cost and increase the uptime and gain more precise customers feedback. Moreover, he thinks it is the time to rethink the strategies because adding sensors will not make a difference but make that data available for analysis will allow customers to pay off for the new the models. In the era of 1980s, manufacturing industry was considerably big as compared to today. By using IIoT, ‘One can still bring a lot of that industry back’, stated by Richard Mark Soley, executive director of the Industrial Internet Consortium (IIC) [8, 9].

Companies that use IoT to increase the productivity, feedback of system and gain customer experience are listed below.

- ❖ **Schneider Electric:** French based global manufacturing company, which allows other manufacturers to increase production by using analytics and modernize the factory floor. Senior Vice President of Schneider Electric said, only way to increase the production and for better decision making is to have precise and sufficient data collected from production floor and make analysis on it [8]. This will allow for better understanding, which plant needs to ramp up and which to shut down. Analysis on real time stream of data can allow management to react quickly. Schneider Electric provides internet enabled smart drives, which when connected to industrial pumps transmits data to central server or cloud. From that data, engineers can forecast the life of pump and reduce the down time of system by doing maintenance, without wasting time on finding the problem. Vice president also said, *“Research shows that in a 10-hour shift, maintenance workers only spend 2.5 of those hours actually working on the equipment; the rest of the time is spent driving to and from the site and hunting down manuals [8].”*
- ❖ **California Oil and Gas Company:** This oil and gas company integrated their system with 21,000 sensors and collect data 90 times in a data. Total data readings they receive per day are around 18.9 million readings. To implement this system, this company spends around 30 million USD. Company estimates that they save around 500 USD per day by increasing up time of single well and 145,000 USD in term of cost avoidance per month per field. [6]
- ❖ **US Water Municipality:** They get data of around 15.84 readings daily. For that purpose they integrated 66,000 sensors in there network. They spend around 18 million USD on this system and expected life of integrated sensors is 17 years. In this case, investment is not only to save the cost leakage, but also for security purpose.
- ❖ **General Electric (GE):** In 2015, GE acquired Current, a new company of data analytics, which is trying to use IIoT for the energy management. Current integrates GE’s renewable energy systems into one company. [8]. GE also teamed up with Cisco for secure big data storage environment centers. Alliance of these two giants, will allow them to provide secure digital industrial solution and big data analytics. Aim of GE is enter in the list of top ten software companies by 2020, said by GE CEO. [10]
- ❖ **Bosch:** It is known for the consumer home appliances. Bosch is providing several IoT services to customers in order to implement desired solution. Some of the IoT services are Bosch IoT Analytics, Bosch IoT Hub, Bosch [9] IoT Integrations, Bosch IoT Permissions, Bosch IoT Remote Manager, Bosch IoT Rollouts, and Bosch IoT Things. Recently, Bosch has launched its IoT cloud, which is only in the testing phase. Bosch is planning to connect all of its devices to cloud by 2020. [8, 10]

- ❖ **Siemens:** It is known for its medical equipment's. Siemens is trying to connect its devices to internet, for that purpose, it tries to make alliance with SAP, in order to provide analysis. [9]

There are many other companies who are using IoT in order to compete in market like Samsung, Qualcomm, PTC, Oracle, Microsoft, Intel, IBM, Huawei, Hitachi, Google, Dell and many others. But the domain of their usability of IoT is not the domain of this paper. All the big companies are shifting their research trend to IIoT. But for small and medium sized enterprises, it is difficult to invest highly on IIoT, despite the fact that it is the need of time. Over 200 million small and medium sized enterprises are in the world this is a good market segment.

3. RESEARCH METHODOLOGIES AND MATERIAL

The main aim of this paper is to provide a cost efficient, highly scalable, easy to adapt and standardized IIoT solution for small and medium sized enterprises. This chapter explains the criteria require to evaluate the suitability of concept of IIoT for an organization. In order to achieve the goal, there is need of Solution of these questions can be achieved by doing research on following topics

- What are the commercials IoT hardwares available?
- What are the current IIoT standards and how they can be followed?
- What are the commercials IoT cloud platforms available?
- What are IoT protocols and how to choose their suitability for an organization?

3.1 IoT Hardwares

IoT is network of highly dynamic and distributed systems that will not only allow the systems present in network to communicate with each other but also allow the end users identification with these smart objects. Any hardware, which has ability to transmit the incoming data to another platform, is considered as IoT hardware. These hardwares when connected with other devices allow them to trigger actions as well as maximize comfort, safety, security and energy-savings [11]. Usually these hardwares are used to collect sensor or machine data and send them to other machines, local servers or clouds using different wired or wireless protocols.

There are several factors which may be taken care while selecting hardwares for IoT devices, some of them are briefed and listed below.

- A. **Size:** With other specifications, size of hardware matters a lot in development of IoT products. Usually smaller physical components are used in scenarios, where network consists of several nodes.
- B. **Cost:** Another factor is to collect information from most possible places in network without additional cost or budget. If per unit price decreases, it is possible to purchase more hardwares, which will eventually help in collecting highly dense data within network.

- C. **Power Consumption:** In order to run for long period of time, it is proposed to use hardware with low power consumption. On factory floor, power is not an issue but if system needs to be deployed in some remote area then factor is power is essential to be considered. For this purpose, hybrid distributed system is introduced, where data is gathered from distributed systems or multiple node and transmit the result of sensor network through one node [12].
- D. **Memory:** It is also important to have sufficient memory in device so that it can run algorithms, programs as well as perform transmission of data collected from different nodes.
- E. **Flexibility:** Hardware must be flexible so that single hardware can be reusable for wide range of applications. It is also important that hardware can be easily integrated with hardware and software components.
- F. **Operating System:** For the implementation of some system that needs to transmit data, it is important for selected hardware to have some well supported operating system by community. The operating system must also support powerful programming languages like java, C, python and JavaScript. Operating systems differ from approach from memory detection to real time features [13]. Some of the famous operating systems supported by IoT Hardwares are Debian, Fedoram Remix, Arch Linux and windows iot.
- G. **Communication:** For IoT devices, it is important to have some gateway through which it can communicate with other devices. Medium of communication may be one or more from Bluetooth, WiFi or even connectivity through Ethernet port.
- H. **Processing Power:** It totally depends on product as well as of application running in IoT hardware that how much power it requires. Some of the IoT devices runs requires very little processing power as well as memory but usually on factory floor, amount and frequency of data that needs to be transmitted is large, where high processing power plays vital role by restricting compromise on any data processing to minimum.

Comparison between different hardwares is listed in Table 3.1.

Features	C.H.I.P	Mediatek Linkit One	Particle Photon	Tesla 1	Adafruit Flora	Light Blue Bean	Udoo Neo	Intel Edison	Raspberry Pi 3	Arduino Yun	ESP 8266
<i>Processor</i>	1 GHz	260 MHz	120 MHz	580 MHz	8 MHz		1 GHz	dual core	1.2 GHz	400 MHz	80 MHz
<i>RAM</i>	512 MB	16 MB	128 KB	64 MB		32 KB	512MB-1 GB	4 GB	1 GB	64 MB	96 KB
<i>Wi-Fi</i>	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
<i>Bluetooth</i>	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗
<i>GPS</i>	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
<i>GSM/GPRS</i>	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
<i>UART</i>	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
<i>I2C</i>	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓
<i>Ethernet Port</i>	✗	✗	✗	✓	✗	✗	✓	✗	✓	✓	✗
<i>SPI Bus</i>	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓
<i>CAN bus</i>	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
<i>SSH</i>	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗
<i>ADC</i>	✓		✗		✗	✗	✓	✗	✗	✓	✓
<i>SD Card Interface/Slot</i>	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗
<i>HDMI Slot</i>	✗		✗	✗	✗	✗	✓	✗	✓	✗	✗
<i>GPIO Pins</i>	8	19	13	16	5	8-16	55	26	40	20	12
<i>Open Source</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>External Power Require</i>	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
<i>Price (USD)</i>	9	59	19	44	20	30	65	70	35	60	4

Table 3.1: Hardware Comparison [14] [15] [16]

All of the above mentioned microcontrollers are commonly used for different purposes in industry from fabrication to industrial process control, depending on the application. Comparison is done by using only on board specifications and functionalities. These functionalities can be increased by using external shields, boards and connectors. Almost all the controllers have WiFi connectivity, which makes it easy to access them from anywhere. Moreover, the decision of hardware is very fatal in long run because there might come a time when one needs to increase the functionality of system by changing the computational power. It is important to make the decision beforehand

depending on communication protocols and cloud services. Data analytics is another important factor, for that, microcontroller must be of high computational power. But if someone need it for connectivity that factors of price and size are on high priority. System security is another main issue in IoT that can be handled by using different encryption certifications. SSL certificates and block chain methods are top in that list.

3.2 IoT Networks

While designing IoT application on industrial scale (IIoT), following are key design considerations that might be in mind.

- **Energy:** The power allows the system to up and running, and how long a IoT device will be in operation with limited supply of power.
- **Latency:** Time require to process, propagate and transmit the message.
- **Throughput:** Maximum amount of data that can be transmitted over the network.
- **Scalability:** Reaction of overall system, when device is added and how much more devices a system can support:
- **Topology:** How different devices communicate and what would be connection between them.
- **Security:** How secure the system/application is.

The importance of these factors varies from application to application. In industry, energy is not a problem but in portable devices it is the main factor. Similarly, on larger scales, security is also a big problem because no one wants to publish its data to its rival/competitors.

There are architectures proposed for IoT systems but each of those was for different domains. Like OSI model, the most general IoT system is also divided into four layered architecture that could be applicable in all sort of applications.

1. **Sensing Layer:** The main objective of this layer is to connect and interact with hardwares to collect data.
2. **Networking Layer:** In this layer, data is transmitted through different networking protocols and support.
3. **Service Layer:** In this layer, different services and business logics are created, which are there for fulfill the user requirements and needs.

4. **Interface Layer:** If we compare whole architecture with OSI model, than this layer is an application layer, which provides methods for interaction between end user and other applications.

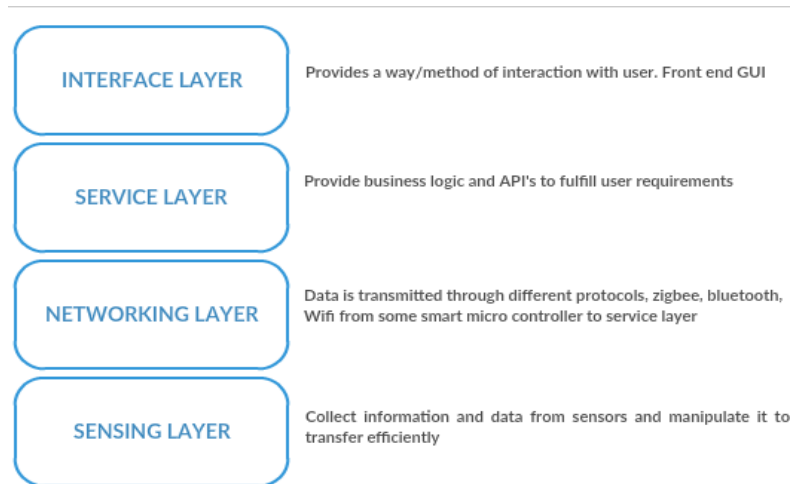


Figure 3.1: General four layer IoT application architecture

Designer of IoT applications has several choices in selecting standards and protocols. These protocols are divided into two categories

1. Short Range Communication
2. Long Range Communication

There are many different communication protocols and standards but some of them, which gains importance in field of IoT, are discussed in this chapter.

3.2.1 IEEE 802.15.4 and ZigBee

In May 2003, ZigBee a short-range data, duplex wireless communication protocol was designed for low complexity and low-cost applications. ZigBee was designed to be suitable for portable or mobile devices. Physical and link layer of ZigBee was designed according to IEEE 802.15.4 standard, for low-data-rate monitor, control applications and low power consumption uses. It is the largest standard for low-data-rate WPANs (Wireless Personal Area Networks). The application layer and network layer of this protocol was designed and developed by ZigBee Alliance in 2002.

ZigBee is sub-categorized, according to its use in different geographical regions

- 802.15.4a/b, recent updates and enhancements and this is published as with 802.15.4c for China
- 802.15.4d for Japan

- 802.15.4e for industrial applications
- 802.15.4f for active RFID (battery powered)
- 802.15.4g for smart utility networks (SUNs) for monitoring the Smart Grid.

There are some variations in all of the above mentioned protocols but base technology is same as defined in 802.15.4a/b. ZigBee has a maximum transmission speed of 250 kbps. It can be used in an application where lot of devices is engaged in little data traffic. ZigBee can mainly transmit data to short distance at not very high transmission rate. IEEE 802.15.4 standard also have possibility of implementing star, cluster and mesh networks as topologies. Among all three topologies mesh is the most reliable and has long coverage range. Mesh provides more than one path for any wireless links.

In any ZigBee network, there are three ZigBee devices.

1. **PAN coordinator:** Only one coordinator in whole network, responsible for trigger/start the network and allow all the devices to bind together. It provides a way to route data between devices. It is main powered device.
2. **Router:** It listens and scans to available networks to join them. Once it gets connected, it transfers data between two devices or nodes. It is also a powered device.
3. **End Device:** It is battery powered device which cannot start in communication or networking however it has tendency to scan and join network.

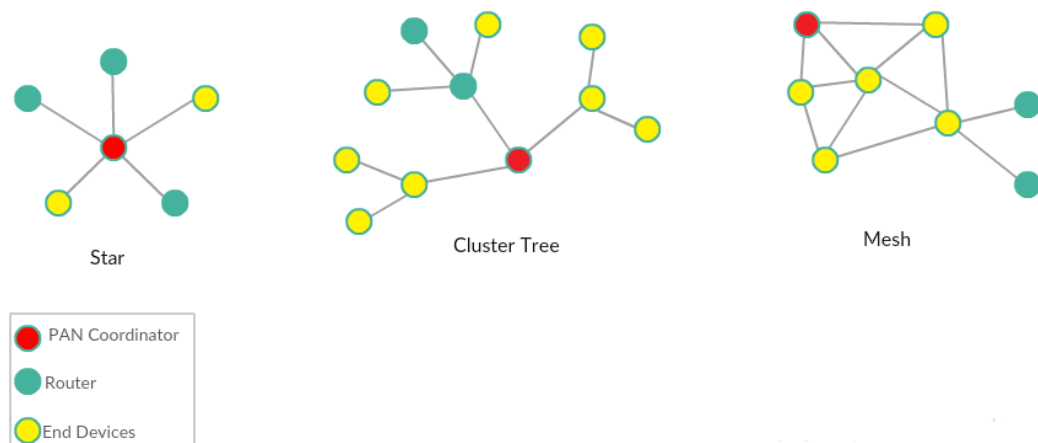


Figure 3.2: ZigBee Network Topologies

The application of ZigBee sensor network includes instrument measurement, physical distribution management, and lightning control, air-conditioning control, monitoring and control of home appliances.

ZigBee works at frequency of 2.4 GHz ISM frequency. Its applications are used globally. It offers a 128 bits AES encryption. ZigBee is mostly used in the mesh application where user wants to increase the connectivity of devices. Wireless sensor network is the most common use of this technology [17].

Advantages

There are several advantages of ZigBee, but the major among all is that it each node can communicate with any node in a network, despite the fact both node lies in range of each other. If nodes are not in range of other node then communication or transmission of data is completed by indirect route through multiple additional nodes [18].

Another feature of ZigBee is scalability. Network can add as many devices as user wants. The only thing that needs to be taken care of is to place two devices in range of ten meters so that end node can communicate to other nodes. Robustness is also a significant specification of ZigBee protocol.

Disadvantages

In order to operate ZigBee compliant devices, knowledge of system is essential. If not encrypted properly, ZigBee communication is also open to attack from unauthorized person like other wireless communications. Range or coverage of ZigBee is limited so it cannot be operated from long distances and hence use of this protocol is not recommended in outdoor.

In order to reduce the transmission rate or frequency of data transmitted to cloud, all the data is sent to single node, which increases the overall latency in system, when ZigBee communication is used. ZigBee protocol is scalable but still network planning is required to overall latency issues. [17]

3.2.2 IEEE 802.15.1 Bluetooth and Bluetooth LE

In 1994, Ericsson developed a new communication protocol and named it as “Bluetooth”. Bluetooth is also a short range communication protocol, which operates at a frequency of 2.4 GHz. Data exchanged between devices taken place after splitting of data in one of the 79 designated Bluetooth channels, each of which operated at 1 MHz frequency. Bluetooth uses UHF radio waves for data transmission [19] [20]. The main objective of Bluetooth development was to have continuous, streaming data applications. It forms a personal area network while communicating with other devices.

A new feature of Bluetooth low energy (BLE) has been revealed in Bluetooth 4.0 version. Design of this new technology makes it suitable for ultra-low power applications. At physical layer, it is almost same as compared to previous versions but communication channel reduces from 79 to 40. The data rate of BLE is 1 Mbps. [21].

It is a bidirectional communication protocol between two or more devices. It is a master and slave protocol in which one device, which establishes connection by initiating the transmission message (Connection Request) to each device are known as masters. Slave is the device which sends the signal of its ability to connect. Several slaves can be connected to single master device. On the other hand, slave can connect with only one single master. Bluetooth LE is based on star topology in which connection time between master and slave is established in 3 milliseconds. Connection request message is used as a reference for synchronization between two devices. BLE has several specifications, which makes it suitable to become standard of low power applications in future. [22]

Bluetooth uses spectrum spreading at the physical layer, which means that data rate transmitted, is much less than the bandwidth occupied by the signal over air. The technique of spectrum spreading allows the Bluetooth to establish low data rate wireless connection without interfering. Bluetooth can be used for IoT devices over the internet using Wi-Fi and home router or access points. Each home has internet access, which can be connected with the Bluetooth enabled router gateway. This gateway is connected with both Bluetooth enabled devices as well as with Wi-Fi access points are connected over WLAN and access point is connected with the internet.

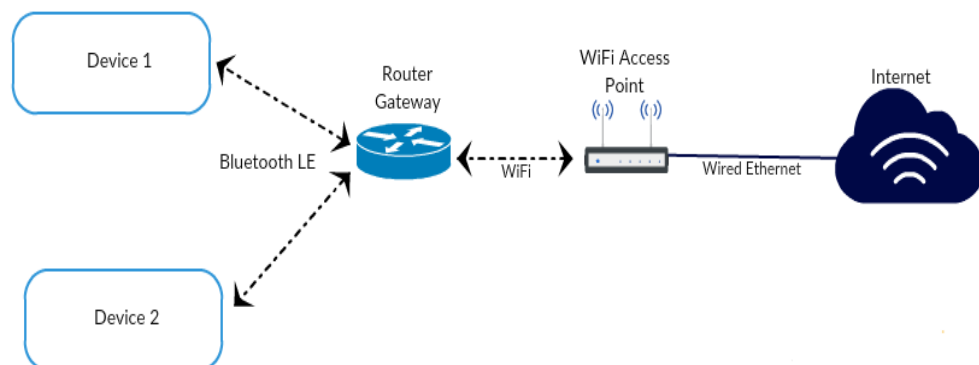


Figure 3.3: Connectivity of devices with fixed Bluetooth LE gateway [23]

Advantages

Bluetooth is a good choice for short range mobile communication devices. It is mostly used for identification, pairing and communication between two devices. Due to worldwide certification, it is compatible with all the devices having feature of Bluetooth in them. Fully automatic feature allows Bluetooth to sense all the other nearby devices. Bluetooth is low power medium of communication so it is used for battery saving and optimization [24]. It also supports password protection authorization.

Disadvantages

Bluetooth operates at low bandwidth and is only useful for short range communication. It is energy-efficient, which makes Bluetooth to send data comparably slower as com-

pared to other communication protocols. Bluetooth 4.0 or BLE only intends to transmit data at the rate of 26 megabits per second, which is much higher than conventional Bluetooth technology.

3.2.3 IEEE 802.11 WLAN/Wi-Fi

Another IEEE communication protocol that operates within ISM radio bands range is Wi-Fi also known as Wireless Area Network (WLAN). Different IEEE 802.11 standards use different bandwidths. Some of them are in table 3.2.

Standards	Bandwidths
IEEE 802.11b/g	2.4 GHz
IEEE 802.11a	5 GHz
IEEE 802.11n	MIMO Mechanism use both 2.4,5 GHz

Table 3.2: WLAN Standards and Bandwidths

This standard protocol operates in as in two modes, ad-hoc mode (p2p) or infrastructure mode (peer to access point). [25].

Infrastructure mode: In this type of connection, a wireless station is connected with an access point and group of these two devices is called a Basic Service Set. Wireless station has the ability to connect with external network (internet) through access point. Service Set ID (SSID) is used for the identification of access point. Several access points connects with a distributed system, in order to connect with other access point through external service set (ESS).

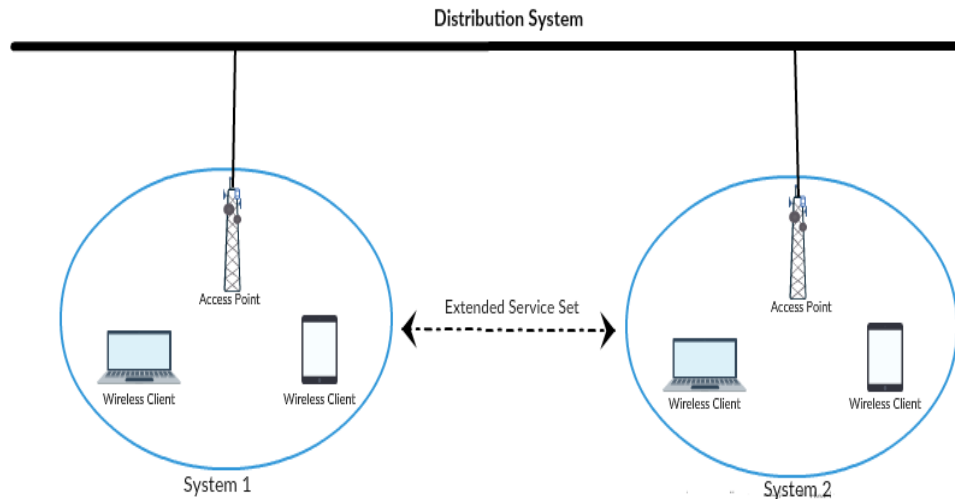


Figure 3.4: WLAN Infrastructure [26]

Then, these access points provide wireless data connectivity to wireless clients. Service set ID is the MAC (Media Access Control) address of an AP, thus SSID allow the wireless station to identify its access point because of unique MAC address of Access point. In order to build a connection with access point, station must pass three steps.

- 1) Scan: When station is power on or wakes up, it discovers a nearby access point by using passive or active scan. Passive scan includes listening to each channel for broadcast beacons sent from Aps. In an active scan, station broadcast the connection request through designated channels and waits for the response from access point on that channel. Once the discovery of access points is complete, station choose one of the AP from list. [27]

- 2) Authentication: After selection of access point, process authentication starts, station sends the authentication frame for the secure connection with access point. Access point responds by sending additional authentication frame to request. This process is done by using network access control mechanism. [27]

- 3) Association phase: After authentication, process moves to association phase. Station sends association frame with data packet and access point responds with additional association frame. Then station sends acknowledgement frame. Once, access point receives acknowledgement frame, association completes and connection is established between station and access point. [27]

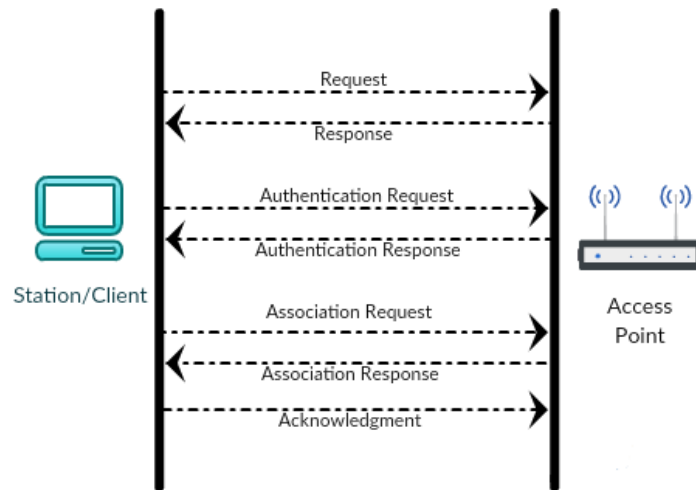


Figure 3.5: Connection establishment between Station (client) and Access Point [27]

Network in which devices or station are connected with access point are known as cells/ Range of network can be increased by connecting several cells with one another. In order to connect cells, they must be in a range of each other, in other words, cells must overlap.

Advantages

Installation of WLAN or WiFi network is quite fast and simple as compared to other network protocols. In WLAN or WiFi, transmitters send data to receivers. Due to which, this protocol is most feasible in scenarios where broadcasting is needed. All the nodes connected to same network broadcast the data to its neighbor as well as to central node, which afterwards send data to cloud.

Another feature of WLAN is mobility. Mobility allows user to have an access of real-time information without restricting the user to single location as far as user is in range of network. As WiFi spreads almost everywhere, so user can retrieve data from anywhere in world. Moreover, WLAN provides service opportunities which promotes flexibility and supports productivity [28].

Disadvantages

One of the major concern with WLAN or with WiFi is security. In case of WLAN, within network then every device is accessible. So if someone succeeds in entering into network, then all the data is visible to that freeloader. Similarly in case of WiFi, data protection is more important because it is open to all. WLAN uses radio signals, so it is susceptible to inference to other devices.

As compared to other network communication protocols, WLAN transmitters consume most power. Therefore, battery life of device with this feature can be adversely impacted [29]. WLAN receivers also limits number of users connected with it. This restriction is still far more than restriction of BLE. Normally a home WLAN router can connect maximum of 25 devices.

3.2.4 Near Field Communication (NFC)

Transport market needs a communication protocol which can be used to feed data remotely from short range by inductive coupling. In 2004, electronic ticketing based communication protocol was developed and standardized and named it as near field communication (NFC) [30]. Later, NFC was used by banking sector for transactions, mobile devices to share data (in safer and more convenient manner to make transmission speedier) and by grocery chains to keep the track record of products in shelves. Now-a-days, mobile phone manufacturers are using this technology to provide leverage to the end users.

NFC supports radio frequency communication which can transmit data at rate of 424 kilobits per second. Moreover, NFC also uses modulation schemes like Amplitude Shift Keying (ASK), load modulation and coding modulation. NFC operates on three different modes which is also shown in figure

1. **Passive Mode:** In this mode, NFC devices act as RFID cards.
2. **Active Mode:** Here, NFC acts as a card reader to read or write the information.
3. **Peer to peer Mode:** This mode allows two NFC devices to exchange data. P2P mode requires less power, because target device uses its own power supply.

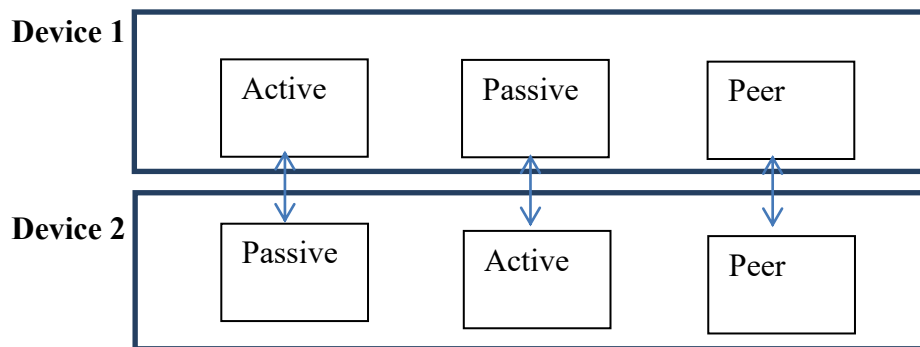


Figure 3.6: NFC: Different modes of operation [31]

Advantages

It is very convenient for non-technical end users to use this technology because data transmission is completed by touching two devices. NFC is also versatile in a sense, it covers industries ranging from banking to restaurants (reserving a seat) and booking

passes. Security is another key feature of this technology because it is safer to transmit data directly to other devices, instead of broadcasting it to local or open network. [32]

Disadvantages

It is considered as expensive to adopt this technology for companies. For small to medium sizes enterprises (SME), maintaining their financial turnover and enabling NFC at the same time is quite a task. Most of the smart devices are embedded with NFC, on the other hand, SME are not ready to integrate NFC with their current system. Another disadvantage is absence of bi-directional communication, when used over web [33].

3.2.5 Z-Wave

In 2001, Denmark based company Zensys designed and developed a protocol explicitly for home control applications and named it Z-Wave [34]. It is a master-slave protocol, where several nodes act as slaves and these slaves transmits data to master. There must be at the most one master in network. Z-wave can form either a mesh or ring network depending on architecture and topology of overall system. There are also routing slaves, which allows other nodes to transmit data.

Single network can contain maximum of 232 Z-Wave enabled devices but manufacturers recommend using no more than 30-50 Z-Wave enabled devices in a network. On average, devices in Z-Wave enabled network communicate after 5-15 minutes with payload of 6-8 bytes. Moreover, this technology takes 200 milliseconds or more to transmit one message.

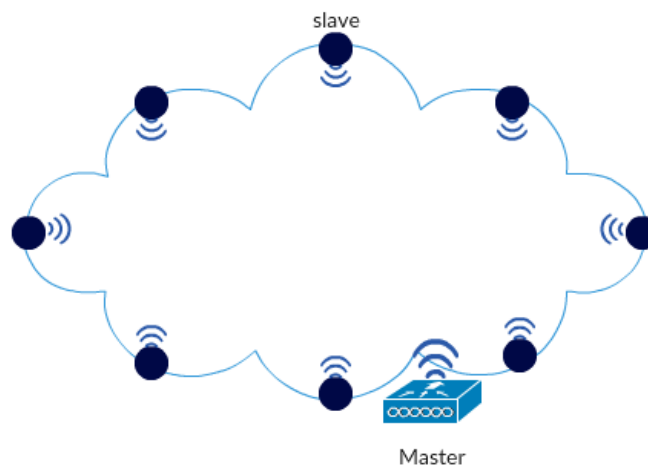


Figure 3.7: Z-Wave wireless network architecture [35]

In US and Europe, Z-Wave use frequencies of 908.42 MHz and 868.42 MHz respectively. Z-Wave use Source Routing Algorithm (SRA) to route messages in network. This algorithm requires arrangement of devices in network with respect to initiator device. In order to keep the cost of implementation low, Z-Wave can be implemented on all the

low cost devices or slaves, which cannot initiate messages but act as a route or slave with only capability to visualize the information of network. Each Message of Z-Wave, which can be routed in a network, requires 12 bytes. It includes routing, frame acknowledgement, collision avoidance with checksum for retransmission of message.

Z-Wave is 4 layer protocol based on OSI model as illustrated in figure. Starting from bottom, MAC layer controls radio frequency (RF) media. Then there is Transfer layer, which handle frames, acknowledgements and retransmission. Second is Routing Layer, which plays role in controlling routes from slaves to master. Upper most layer is Application layer, which allows transmission of payload and receiving frames.

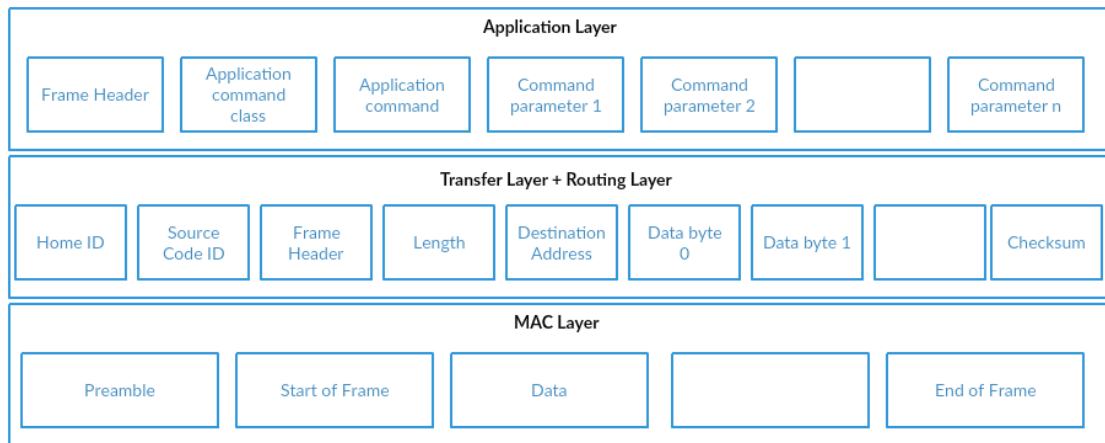


Figure 3.8: Z-Wave protocol four layer OSI model [36]

The other two main features of Z-Wave is self-healing and self-organization. Self-organization allows Z-Wave devices to discover all the neighbor slave nodes as well as master. If any of the node in network is unavailable, self-healing capability allows devices to generate new dynamically routes. These two features are part of Z-Wave software, which lies in on-chip memory.

Advantages

It is easy to set up Z-Wave network, due to its feature of scalability, it is also easy to add or remove devices in existing network. In addition to this, Z-Wave consumes less power and hence reduces battery usage. Devices compatible with Z-Wave can be operate able with other remote devices, which provide continence to users. In terms of security, Z-Wave provides support for AES 128 type of encryption. Z-wave technology is cheaper as compared to other technologies of this domain, so it is affordable to use this technology in products.

Disadvantages

Due to limited coverage of Z-Wave, it increases the cost of network setup, when whole system will be deployed for larger area. This technology also only follows tree struc-

ture, which limits the options for implementation. Further, due to low speed and small data size communication, this technology can only be used for monitoring and control purposes.

3.2.6 Comparison between IoT network layer protocols

Selection of IoT network layer protocols merely depends on application, specification of overall system, end user demands, methodology designed for system and compatibility of network layer protocol with upper layer protocols. Table 3.3 represents some of the major factors which will allow designer to compare and select one or several protocols for IoT application.

Standard	ZigBee	Bluetooth	Z-Wave	NFC	Wi-Fi
IEEE	802.15.4	802.15.1	ITU-T	IOS 13157	802.11 a/b/c/g/h
Frequency Bandwidth	868,915 MHz,2.4 GHz	2.4-2.5 GHz	908.42 MHz	13.56 MHz	2.4GHz, 5GHz
Channel Bandwidth	2 and 5 MHz	2 MHz			20,40,80 MHz
Maximum Signal Rate	250 Kb/s	305 Kb/s	40 Kb/s, 100Kb/s	424 Kb/s	54 Mb/s
Range	10m	~50m	~30m	~5cm	100m
Cryptography	AES block cipher	AES Encryption	AES Encryption		RC4 stream cipher,WEP,WAP2,AES block cipher
Network Type	WPAN	WPAN	WPAN	P2P	WPAN,P2P
Spreading	DSSS	FHSS	FHSS	GSMA	DSSS,CCK,OFDM
Coexistence mechanism	Dynamic Frequency Hopping	Adaptive Frequency Hopping	Adaptive Frequency Hopping	RFID	Dynamic Frequency Selection, transmit power control (802.1.1h)
Physical Layer data rate	Upto 250 Kbps	1 Mbps			72.2-867 Mbps depending on antennas [2 antennas at 80 MHz channel and 1 antenna at 20 MHz channel]
Power Consumption (mA)	~40 (<10mW)	~12.5(<10mW)	2.5	~50	~116 (@1.8V) (>100mW)

Table 3.3: Comparison between IoT communcation [27]

3.3 IoT Cloud Platforms:

IoT solutions require a platform where all the data can be gathered from various devices connected in a network. This platform plays important role in optimization of solution. According to Cisco and Gartner, IoT devices will increase to 20-25 billion approximately by 2020 [37].

Selection of IoT cloud platforms must be done after analysis of factors like technical offerings, strategy, market presence, certifications and recommendations. Analysis of technical offerings is important to integrate the current solution to cloud platforms, so that users can access the solution remotely. It includes different use cases, licensing and billing models, application support, hardware and software development kit support and management of solution. Strategy completely depends on company core business domain. Factor of market presence allows comparing between different IoT cloud platform provider services to particular market. Certification and recommendation helps in prediction of maturity level of IoT cloud service provider.

Cloud platform provides following three types of services.

1. ***Software as a Service (SaaS)***: User can take full advantage of pre-processed and pre-defined services by just connecting IoT hardwares with cloud without spending time on configuration and building their own software suits.
2. ***Platform as a Service (PaaS)***: This service is for developers, where cloud platform provides support for software development kit. There is no need to develop application on local machines. This service makes continuous integration of new features in previously build solution quite easily.
3. ***Infrastructure as a Service (IaaS)***: This service only provide data or application storage feature, which is useful to deploy applications and solutions. IaaS eliminates the cost of new servers as well as maintenance cost.

There are more than 49 cloud platforms are available in market, some of them are open source but mostly mature platforms are paid. Advantages and disadvantages of some emerging cloud platforms are following.

- ***KAA***: It provides supports for NoSQL and Big Data base applications. On the other hand, it is not compatible with most of the hardware modules.
- ***Carriots***: It supports event-driven and triggering based applications but this lacks in user interface designs.
- ***Xively***: It was introduced by Gravity Cloud Technology. It allows to integrate hardware modules with minimal effort. Contrarily to this, it lacks notification services.

- **Axeda:** This platform is specially designed for machine to machine data management support. But its major drawback is lack in self sustenance. Moreover, it is dependent on third party we services.
- **Open remote:** It supports open cloud service and is too muck costly for developers to develop data management system over it.
- **ThingWorx:** It was designed by PTC Inc. Main purpose was to provide M2M and IoT support to end user. Development of data intensive applications is remarkably easy using this platform. But only limited number of devices can be connected to this platform.
- **ThingSpeak:** It also provides triggering feature but it can support connection of very few devices at one time.
- **Plotly:** As it name says, Plotly is the best available visualization platform for IoT cloud support. Its disadvantage is that it provides limited storage capacity.

3.3.1 Comparison between mature IoT cloud Platforms

IoT cloud platform should provide support for more than one domain and use case structure, so that it can facilitate several solutions simultaneously without shifting to other platform for different scenario. While selecting any IoT cloud platform, it is important to consider billing model because these payment models based on number of request send by client. Selected platform also has ability to provide support for multiple application layer protocols, this will allow any organization to stick with single virtual environment for their products. Besides protocols, platform must provide support to all the famous programming languages as well as hardware's for the sack of communication. Commonly used serialization formats are JSON and XML, in addition to these serialization formats, cloud must provide support for Sigfox to reduce and optimize the traffic. Virtual environment or cloud platform should also provide container based solution to enable firmware installation and OTA support. [38]

Above all the specifications, cloud platform must be able to provide support for scalability, real-time data, bi-directional communication, data analytics, diagnostics, data visualization and last but most importantly security. Starting from scalability, as IoT devices are increasing exponentially, so it is important to have scalable solution to integrate all the devices. Real-event drive or real time data, allows IoT devices to predict the forecasting and data visualization. Bi-directional communication allows user to operate device from anywhere, without bi-directional communication there is no aim or benefit of introducing IoT to current system. Moreover, platform should enable real time and offline analytics capabilities for health logs and data collection. As, volume of data is growing rapidly, platform should also be able to provide support for Big data,

which eventually will allow to store only valuable and meaningful data. It is also important to provide diagnostics feature and infrastructure performance monitoring by the platform. Now-a-days security of data is major concern for all the companies, so it Transport Layer Security (TLS) should also be present by default. Moreover, data encryption and security compliance are the factors should be taken care of during selection process. Table 3.4 shows the comparison between Microsoft Azure, Amazon Web Services and IBM Watson IoT cloud platforms.

	Microsoft	Amazon	IBM
Platform Name	IoT Hub	AWS IoT	IBM Watson IoT
CEM/ERP Integration	Manual	Manual	Manual
Field Service Integration	Manual/Partners	Manual/Partners	Manual/Partners
Visualization	Yes	Yes	Yes
Analytics	Yes	Yes	Yes
Machine Learning	Yes	Yes	
Big Data	Yes	Yes	
Notifications and Alerts	Yes	Yes	
Lifecycle Management	Yes	Yes	Yes
Security	X.509, TLS	X.509	TLS
SDK	Open source	Open Source	
Protocols	AMQP, MQTT, HTTP, WebSockets	MQTT, HTTP, WebSockets	MQTT, HTTP
Device Gateways	Yes	Yes	Yes
Object Storage	Yes	Yes	Yes
Libraries for Small, embedded devices	Yes	Yes	Yes
Access Control Permissions		Yes	

Table 3.4: Comparison between IoT Cloud Platforms

3.4 IoT Application Layer:

The main objective of IoT application is to provide visualization, micro services and scalable solution to end user, so that if some machine is added into the system, the efficiency of whole system remains same. This objective can be achieved by using application layer protocols. There are many different types of protocol available for different

applications. Each of these has their own advantages and disadvantages. Some of the most commonly used and mature application layer protocols are discussed below.

3.4.1 Message Queue Telemetry Transport (MQTT)

It was designed by IBM in 2003 and IBM used it for several years before launching it as open source community. The real aim of MQTT is to reduce the bandwidth requirements. MQTT is a light weight, publish/subscribe protocol based on messaging between clients and broker. It runs over TCP/IP that's why, it is suitable for Machine to Machine (M2M) and IoT applications. It also provides guarantee and reliability of packet transmission and delivery. MQTT provide support for communication between one to many devices. It also has ability to establish secure connection between remote devices.

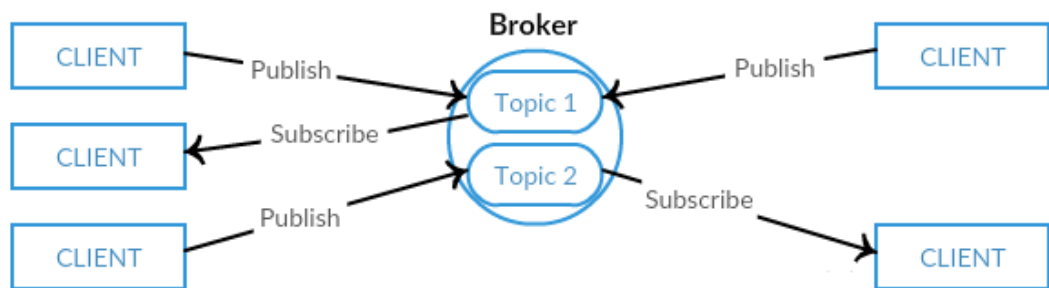


Figure 3.9: MQTT protocol architecture

MQTT also supports three level of Quality of Service (QoS). In QoS0, the delivery of data or message cannot be acknowledged, due to which message could be lost or duplicate, so that this level of service cannot be used to store messages or to make a queue of messages. On the other hand, this QoS could be used to achieve goal of transferring data quickly. QoS1, allows MQTT client to store message locally which enables it to re-transmit message. If message failure occurs before an acknowledgement, client will re-transmit last message. In this case, threat of duplication of messages increases. In QoS2, message stores not only at sender client node but also on receiver client node, which gives guarantee of no message duplication. [39]

MQTT Protocol stack includes Transport Layer which is based on TCP/IP. As explained above, MQTT follows messaging protocol of publishing and subscribing. It is light weight protocol due to presence of IPv6 and 6LoWPAN in Network Layer. MAC and Physical layers are totally designed according to IEEE 802.15.4 standard.

MQTT Publish and subscribe messages contain fields like message type, duplication flag, quality of service, retain, length of topic name, topic name, message ID and payload. In general, MQTT message structure is composed by fixed header, variable header and payload.

Advantages

In IoT systems, response times, throughput, battery-consumption and bandwidth are key factors, which must be consider and taken care of while designing IoT system or device. The main benefit of using MQTT is that it was developed for resource constrained devices (any system or device which runs on battery and has limited storage capacity). MQTT has features of faster response time, lower bandwidth and battery usage. Due to these key factors, it is suitable for use cases where connectivity of recurrent, bandwidth is at premium, application needs to interact with several other devices, reliable data transmission [40]. Flexible Subscription pattern is another feature of MQTT, which means a small monitor can listen to all of the other topics by subscribing to them. Table 3.5 illustrates the advantages of MQTT protocol over conventional HTTPS protocol.

Characteristics		3G		Wi-Fi	
		HTTPS	MQTT	HTTPS	MQTT
Received Messages	Messages/Hour	1,708	160,278	3,628	263,314
	Percentage Battery/Hour	18.43%	16.13%	3.45%	4.23%
	Percentage Battery/Messages	1.709%	0.01%	0.095%	0.02%
	Messages Received (Losses)	240/1024	1024/1024	524/1024	1024/1024
Send Messages	Messages/Hour	1,926	21,685	5,229	23,184
	Percentage Battery/Hour	18.79%	17.80%	5.44%	3.66%
	Percentage Battery/Message	0.975%	0.082%	0.104%	0.16%

Table 3.5: MQTT vs HTTPS [41]

Disadvantages

The problem with MQTT is its transport layer. It is based on TCP connections. TCP connection between client and broker has always on connection, which reduces the time to put to sleep of device [42]. MQTT is lightweight protocol due to which it lacks encryption. Encryption adds significant amount of overhead.

3.4.2 Constrained Application Protocol (CoAP)

For resource constrained devices, it is difficult to connect in secure manner. Another document-transfer protocol for resource constrained internet devices and M2M communication is CoAP. It is based on request/response interaction model for exchanging of messages over UDP transport layer. For the sack of efficient communication, CoAP also use REST interface. As, HTTP use TLS to secure the communication, CoAP use DTLS for security and data encryption. [43]

CoAP provides reliable as well as unreliable mean of communication. In CoAP, devices may act as a client, server or both to other devices. Moreover, CoAP is asynchronous protocol, which means it is connection-less with higher performance, smaller packets and reduced overheads. All these features make it suitable for low-energy consumption applications [44]. CoAP allows IoT device to be discovered and expose it-self to other devices in network by using Uniform Resource Identifier (URI). CoAP is used where direct, responsive and lightweight communication is required.

The concept of raw public keys is used by CoAP for authentication, in which client initiates the communication by configuring and sharing raw public key. Client sends “Hello” message to server. Server search for client identity, verifies it and reply with “Hello_Verify_Req”. Client then, verify the response from server and sends “C_Hello” to server and server replies with “S_Hello”. Then process of Key exchange starts at this point, after which, if server needs client’s authentication, server can send “Certificate Request” to client. This process is shown in figure. [45]

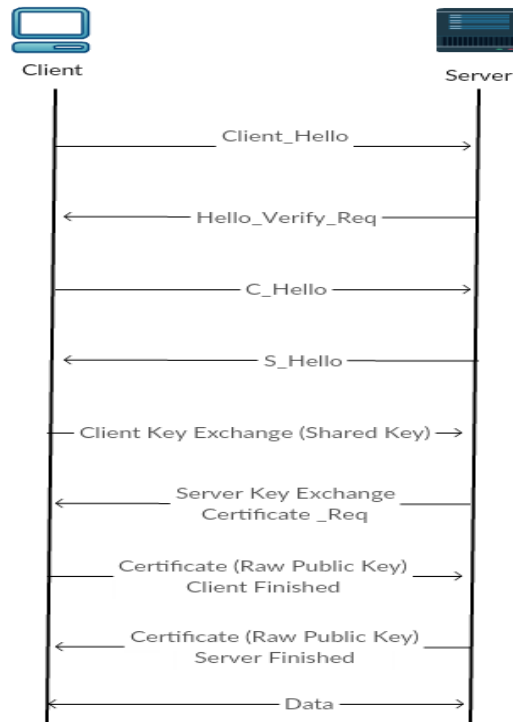


Figure 3.10: CoAP Public Key Sharing

In addition to this, CoAP message is minimum of 4 bytes. All these four bytes are in sort-fixed header. It also has compact binary options and a payload in message. CoAP message packet is shown in figure

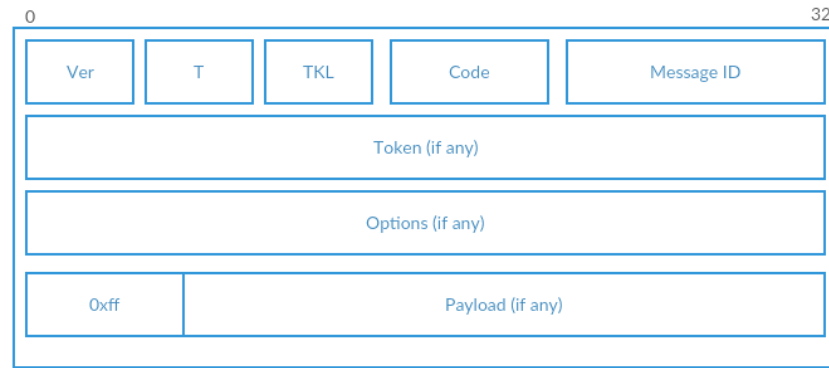


Figure 3.11: CoAP Message Format

Advantages

CoAP is a light-weight and low power consuming protocol, it is good option for low-power sensors. It can be used to work with REST-based API's as well as on top of packet-based technologies. It can also be used in application based on state transfer model. CoAP provides inbuilt support for content negotiation and discovery allowing devices to probe each other to find ways of exchanging data.

Disadvantages

There are no native capabilities of broadcasting messages in CoAP, it is one-to-one protocol. It is not purely event based. CoAP seems to be based on scalable architecture but there are some limitations of UDP usage, which includes lack of advance quality support and port forwarding [46].

3.4.3 Extensible Messaging and Presence Protocol (XMPP):

In 1998, Jabber protocol was built on XML, for instant messaging, which later transforms into XMPP. Like other protocols, XMPP clients with unique name communicate with each other through associated server. During the communication or in transmission of information or data, server is just there to provide routing details. Besides providing routing details, servers can also communicate between different domains to increase network through internet. Figure shows the architecture of XMPP. [47]



Figure 3.12: A simple XMPP architecture with two clients [48]

Model of XMPP is decentralized, which means there may be several servers running within one system or network. It is a text based protocol, which works over TCP or via

HTTP using a WebSocket implementation. XMPP provides a framework not only for instant messaging but also for distribution of Presence data. For security and encryption of data, XMPP uses Transport Layer Security (TLS) and Simple Authentication and Security Layer (SASL).

Like e-mail, XMPP also uses core protocol, in order to create a stream for XML data flow via TCP transmission, which makes it a server less protocol. Besides that, user can have its own XMPP server up and running to manage real-time data exchange.

Advantages

As stated earlier, XMPP is decentralized in nature. Due to this property of XMPP, any user can utilize the servers located closer to its location. Moreover, because of its architectural similarity with e-mail, it is free and easy to understand. This XML based protocol allows user to build customize solution to main permeability. In addition to this, XMPP also supports real-time communication that may be used in network management, file sharing and remote monitoring [49]. XMPP may also be used to diversify the resources and to build distributed systems.

Disadvantages

Practically there is no official support for XMPP clients or server. It is analyzed and observed that almost 60% of data flow in XMPP is repeated because of distributed and decentralized nature. Overhead of data in instant messages between different recipients is also enormous in XMPP. It also does not provide support for modification of binary data. In terms of security, XMPP only supports Base64 data encryption session for types of data (binary, graphics, etc...).

3.4.4 Hyper Text Transfer Protocol (HTTP)

HTTP is a client/server and asymmetric protocol, which works on TCP to provide reliable connection. It is most widely used protocol not just for web applications but also for virtual connection between hardware and software applications. It provides support and integration capability for almost all the programming languages.

HTTP was first proposed by Tim Berners-Lee in 1991. The main goal of HTTP proposal was to have one-line protocol which can be adopted by World Wide Web (www) to provide functionalities like file sharing, index search request, format negotiation and communication with other clients through same server. The period of 1991-1995 was an evolution of HTML specifications where main focus of software development shifted to web applications. Later in May 1996, RFC-1945 which is known as HTTP/1.0 came in.

With the continuous development and experimentation HTTP improves with time and later HTTP/1.1 and HTTP/2.0 were introduced. [50]

In newer version, main aim was to build HTTP on subsets like client request and server response in single ASCII character string, server response in HTML and termination of connection after completion of data transfer. In HTTP, client sends request to server and after authentication of client, server response back. Security was a major issue, which was achieved by encrypting data using SSL certificates and TLS. In order to prevent any data loss, cyclic redundancy check (CRC) was introduced in HTTP. Moreover HTTP also prevents duplication of data. Figure shows the simple client/server communication. [51]



Figure 3.13: HTTP client/server communication

Advantages

Identification is one of the advantages of HTTP. It enables file sharing without questioning sender about type of application required to read or write the content of file. HTTP also enables multiple connections to achieve high transmission of data. Several downloading can be accomplished by using HTTP because it assigns particular file type against each element to handle the communication faster and efficiently. Long serial numbers which actually are IP addresses can be mapped to recognizable names using HTTP [52]. As stated earlier, HTTP use SSL certificates for secure and encrypted communication (HTTPS). The risk of interception also reduces because HTTP opens single connection per data handling (file transferring, data downloading, etc.) and closes that connection immediately after process completion. HTTP also has ability to fetches out data from database with single request. It also has ability of “pipelining”, which means it can open connections for several requests simultaneously.

Disadvantages

HTTP can be used for bi-directional communication but opening and closing of connection takes time with makes it not suitable for real-time communication where frequency of data transmission is so high. Moreover, connection between client and server will not terminate, if client keep it alive. This might increase security risk factor and resources might also be not available to other clients.

3.4.5 Comparison between IoT network layer protocols

While selecting IoT application layer protocols for application or IoT system, there are some factors which are important to take under consideration. Some of the factors are data reliability, frequency of data transmission, connectivity options and support, support provided by different cloud platform for that protocol, how much resources a protocol can use and how much resources can be offered to protocol, data security and under what scenario application layer protocols are required.

It is recommended to select the protocol while designing the system based on required specifications. Table 3.6 represents some of the major factors which will allow designer to compare and select one or several protocols for IoT application.

Features/Protocols	CoAP	MQTT	XMPP	HTTP
Transport Layer supporting Protocol	UDP	TCP	TCP	TCP
Messaging Type	Request/Response Publish/Subscribe	Publish/Subscribe	Request/ Response	Request/Response
Cellular Network Connectivity	Excellent	Excellent	Excellent	Excellent
Low Network Connectivity	Excellent	Fair	Fair	Fair
Cloud Platform Support	Azure (Through Gateway)	Azure/AWS	GCP	Azure/AWS/GCP
Compute Resources(RAM/Flash)	10Ks	10Ks	10Ks	10Ks
Security	DTLS	SSL/TLS	TLS/SSL/XEP-0198	TLS/SSL
Quality of Service (QoS)	Optional (ACK packet from receiver)	3 Levels -At most once -At least once -Exactly once	None	TCP Enabled
Use Cases (Support Environment)	Field utility works	Real Time messaging in IoT applications where bandwidth is at premium	Remote or Distance management of consumer white goods	Large data transfer in Websites or smart energy profiles

Table 3.6: Comparison between application layer protocols [53]

4. PRACTICAL IMPLEMENTATION

This chapter explains one of the famous IIoT framework with selection criteria of all the topics discussed in previous chapter and architectural solution of problems faced by JOT Automation with its working and benefits. In addition to that, proposed architectural solution and other use-cases with different options are also present in this chapter.

4.1 PTC Incorporation Framework

At this is important to discuss the actual IoT framework proposed by PTC Incorporation, which is considered as pioneer in this field. The framework proposed by PTC Inc. from designing and transformation of any product to complete IIoT system is shown in figure 4.1.

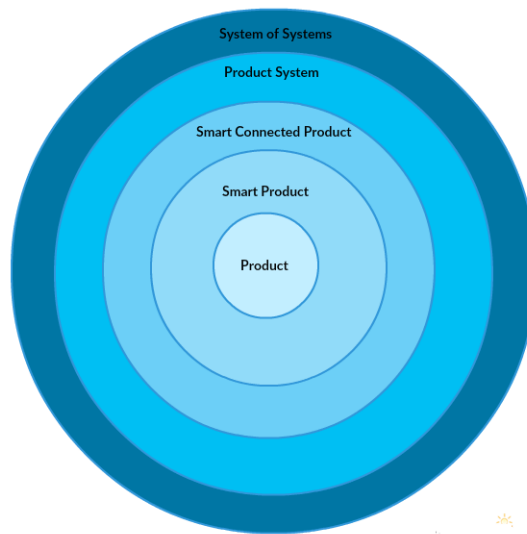


Figure 4.1: IIoT PTC Inc. Framework

Based on this framework, IIoT system is designed for JOT Automation. G3 is the quality test automation machine of JOT. When this product will be connected with any graphical interface and cloud to visualize and storage of data, then simple G3 is converted to Smart Connected G3. Several other machines (M10 box and gaia) or industrial equipment's connected together in same manner to form System of Products. Different System of Products at several geographical positions connected with cloud services to form System of Systems. Figure 4.2 is the visual explanation of PTC Inc. framework in terms of JOT Automation products.

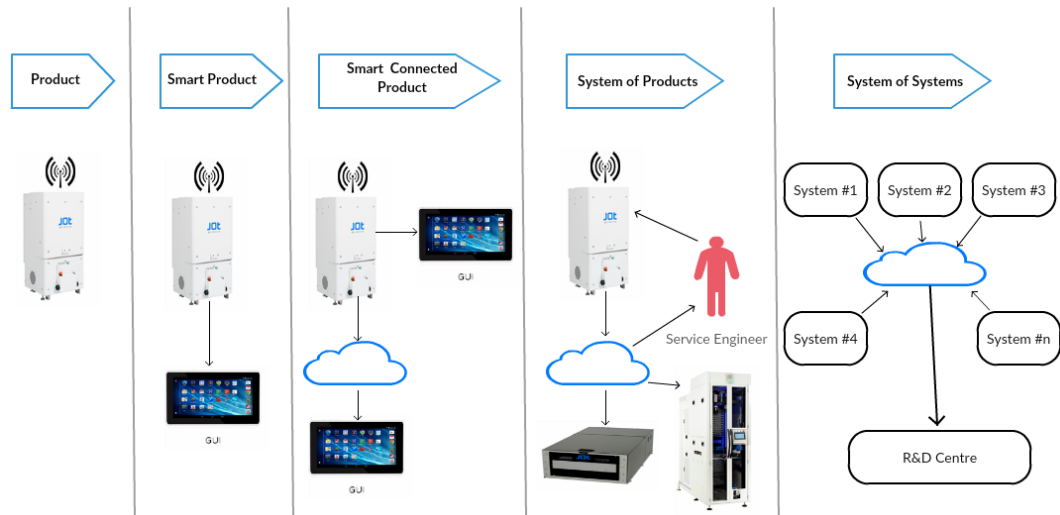


Figure 4.2: JOT Automation IIoT System of Systems

The main benefit of having this sort of framework is providing the concept that how the actual system will look like. Moreover, it also allows engineers to observe and analyze every single detail in designing phase.

4.1.1 Working and benefit of Smart Connected Products

On a factory floor, several smart connected automated production equipments send performance based data to single command center. This command center is embedded with some software, which visualizes the incoming traffic, analyzed it and manipulates it according to pre-defined rules. It is also the responsibility of command center to generate triggering responses and send alerts and notification to onsite technicians. Those technicians are responsible for optimization and maintenance of machines. The flow of data on factor floor is illustrated in figure 4.3.

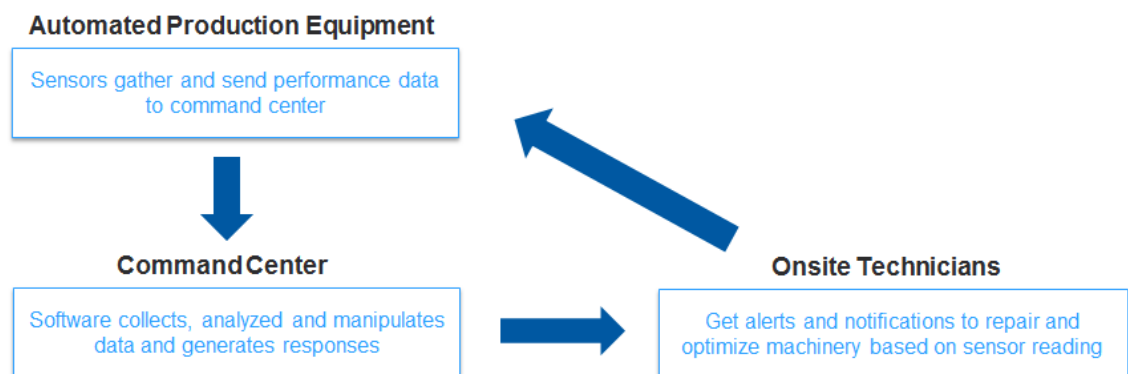


Figure 4.3: IIoT data flow and working on factory floor

4.2 Proposed Architecture

Main problems JOT Automation were facing was how to connect multiple machines (G3, M10 box and Gaia) to IoT network, how to implement basic service counters, statistics and remote control API so that it can be provided to customers, how to connect single machine (remotely and straight) with mobile terminal and how to monitor and visualize the overall status of machines in server view. In other to provide scalable and low-cost solution, architectural solution was proposed which is shown in figure 4.3.

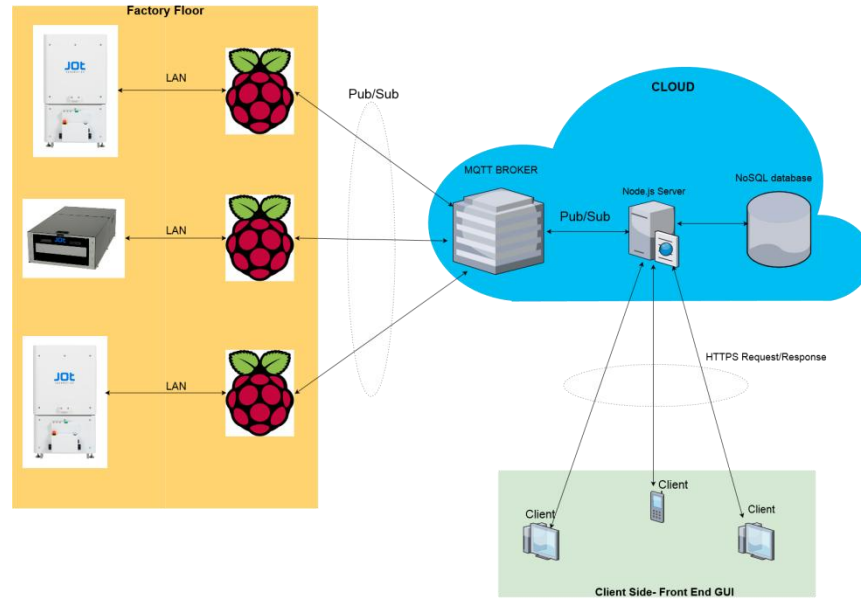


Figure 4.4: Proposed architectural solution

In this proposed architecture, each JOT Automation machine is connected with micro-processor or micro-controller through Ethernet port to gathers data from particular machine. In micro-processor, data is manipulated to transmit only useful data and stores all the information coming directly from machine. After that data will be transmitted to central server which is responsible to control bi-directional communication and to store the data in databases. Amount to incoming data to server again manipulates the information to store the least possible data in order to lower the load on it as several machines are transmitting data simultaneously. For this purpose, several micro-services and RESTful API's are implemented which act as backbone of server. Whenever, client or JOT requests for any data from any machine, server fetches data from database and visualize it on client side. Selection criteria of technologies used for this purpose are explained in next sub-section.

4.3 Selection criteria

Selection of hardware, communication protocols and cloud services completely depends on problem and proposed solution which were explained in chapter 3.

In order to provide scalable and independent solution, Raspberry pi 3 is selected as IoT hardware. The only way of connection with JOT M10 box is through Ethernet port over LAN or CAT 5 cable. M10 box is already embedded with windows server, but to provide independent solution, external hardware was needed. In addition to have an Ethernet port, Raspberry pi 3 is also supported with 1 GB of RAM and Linux based Debian operating system with WiFi and Bluetooth modules. There was also need to have storage capacity in order to save data local to prevent any data lose in case of black out or power cut-off. Raspberry pi 3 supports memory cards and there are four USB ports present which can be used to connect external hard drives. Data sheet of Raspberry pi 3 is in appendices of this paper.

For network layer protocol, WiFi was selected. It was due to the capability of WiFi to transmit data over long distance. Moreover, there was a need to control the JOT machines to control remotely, this can only be achieved by using WiFi. The main advantage of using this protocol is to make each system independent from others. Overall system in this case is distributed.

For application layer protocol, MQTT was chosen with HTTP. This selection was totally based on performance and security features of these two protocols. Moreover, MQTT is most popular and commonly used protocol for IoT devices. It allows to transmit data much faster as compared to other devices. On the other hand, HTTP is widely used protocol for web based applications. It is easy to understand and as most of the systems are already built on HTTP, so it is easy to integrate it with other systems.

AWS was selected to provide cloud support for this overall system. AWS is most matured cloud service provider with benefits of having one year free tier for demonstration purposes. AWS also supports MQTT, HTTP and CoAP which makes it most suitable. Features like IoT hub, IoT container and lambda functions are useful for future development. It also provides support for the deployment of MQTT broker and MEAN stack based applications. Moreover, AWS provides all three kinds of services PaaS, SaaS and IaaS. Support for all the popular languages is another additional feature of AWS. All the selections are based on concerns of future development.

Programming languages used were Python to manipulate data and design payload on Raspberry pi 3 because of large number of built-in library support, Node.js for server side development and web application and NoSQL database for data storage because data coming for each machine is different from other so designing a single schema will not be enough.

4.3.1 Setup

In order to setup whole environment, Raspberry pi 3 needs to have Raspbian Jessie operating system. To setup raspberry pi 3, download raspbian from

<https://www.raspberrypi.org/downloads/raspbian/> . Download raspbian jessie with desktop and mount it on SD card. Insert SD card in slot of raspberry pi and power it up. On first boot, install the operating system from SD card. Once, OS is installed and desktop is displayed, connect raspberry pi with wifi. Then to update the raspbian, open terminal and type following commands.

1. `sudo apt-get update`
2. `sudo apt-get upgrade`
3. `sudo apt-get install pip`
4. `sudo chown -R $USER /usr/local/lib/python2.7/dist-packages`

Command 4 gives access to root directory. Only Ethernet port and three GPIO pins are being used. GPIO 4 supports one wire protocol and used for temperature sensors. GPIO 18 and GPIO 24 are connected with LED's to display warning and connection status interrupts respectively. Figure 4.5 shows hardware setup.

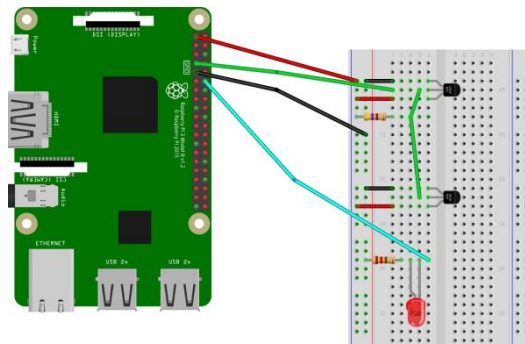


Figure 4.5: Hardware setup

As, data is coming from more than one source so there is need to construct payload. Moreover, data is changing frequently so that there is only delay of five seconds between sending two messages. Following lines of code show construction of payload.

```

0. client.loop_start()
1. while 1:
2.     values.counter+=1
3.     location=values.location
4.     send_msg = {
5.         'client':values.client,
6.         'name': values.name,
7.         'counter': values.counter,
8.         'serial': values.serial,
9.         'location': values.location,
10.        'serviceInterval': values.serviceInterval
11.    }
12.    client.publish(config.pubTopic, payload=json.dumps(send_msg),
    qos=2, retain=False)
13.    data = [1, values.name, values.counter, values.serial, val
    ues.location,values.serviceInterval,values.client]
14.    retain.writeData(data)
15.    time.sleep(5)
16. client.loop_forever()

```

Warning interrupts are based on value of serial counter (current counter value) and service interval (maximum number of counter a particular part can count). There is check on server which sends signal back to Raspberry pi 3 and turns on Warning LED, when serial counter reaches to 80% of service interval value. Moreover, predictive time is calculated based on following formula

$$\text{Predictive maintainanace time} = \text{current time} + (\text{service interval} * 80\%)$$

Line 12 of code is message publishing command whereas line 15 allows the program to save the current data in excel file so data overall system restarts from last saved counter values.

4.4 Different Options and Use-cases

There are several limitations and restrictions on factory floor due to security. Some factory floors have access to internet while others only have WLAN connectivity. In some cases there are no wireless mean of communication. In order to provide wider view of IIoT, there is need to have more than one solution, which can deal with any scenarios.

First option is similar to what was implemented earlier, in which several JOT machines are connected with central server located in cloud and responsible for storage of data and visualization of information in meaningful manner. Figure 4.5 illustrates first option.

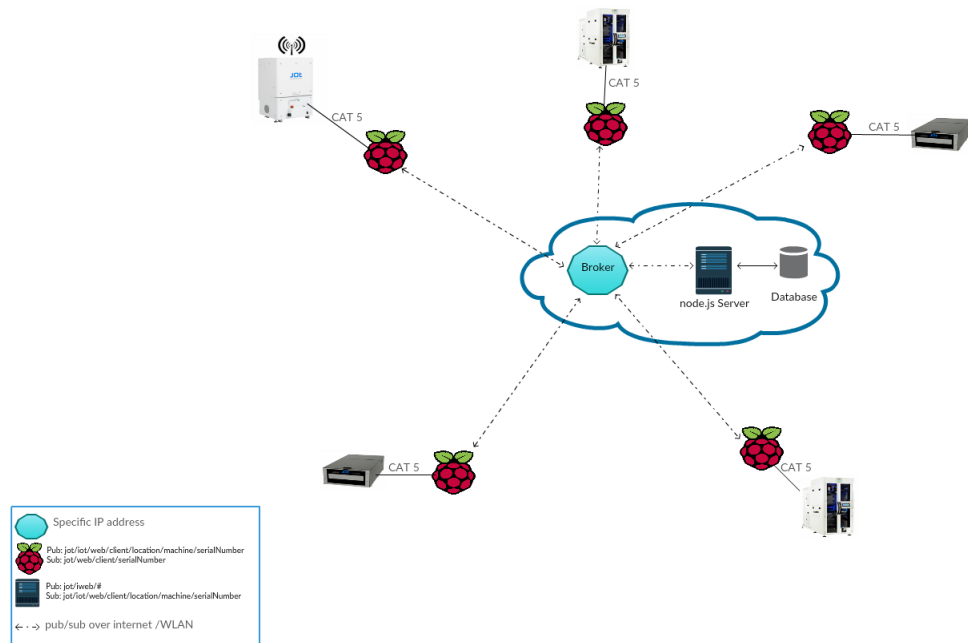


Figure 4.6: IIoT Option 1

This approach can be used as distributed as each machine act as independent source and if central server fails under worst case scenario than data can be retrieved back from micro-processor. Option 1 also works under three following scenarios.

1. If no internet connectivity is present but WLAN connection is there to serve then broker, server and database will be deployed in separate raspberry pi 3 which will act as a local cloud. In this case, IP of raspberry pi 3 must be static. This can be achieved by port forwarding in WLAN connection.
2. If there is no WLAN connection, then deploying a simple router will do the task. But range of router must cover each and every raspberry pi 3 to include them in network.
3. If internet connection is present then broker, server and database will be deployed in cloud.

Option 2 is quite different in terms of technology, which follow conventional industrial standard of having one central server. But medium of communication for data flow is wireless through ZigBee. Where Xbee modules are connected with each machine and PAN coordinator is connected with MEC server. Xbee's modules act as single node to communicate with each other to form a mesh where every node helps other to transmit data to MEC server. Providing internet connectivity MEC Server will transmit data to cloud which can visualized later. General idea of data flow from factory floor to end user remains same through cloud services. Figure 4.6 reflects the idea of option 2 using ZigBee connectivity.

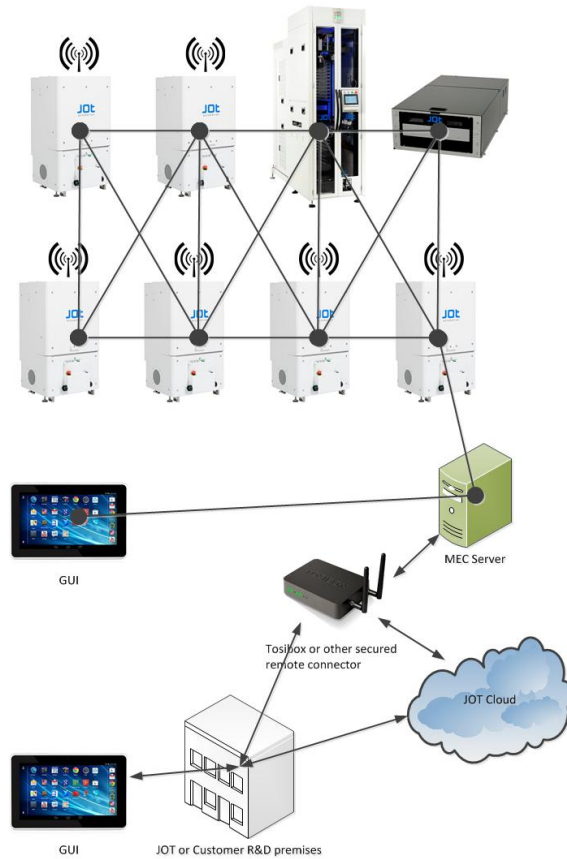


Figure 4.7: Option 2 using ZigBee connectivity to form mesh for data transmission

The overall topology of system remains same in both cases which would be star of stars, where several systems connected together to provide continuous feedback at same node. Live monitoring can be achieved by using this system. Figure 4.7 shows system of systems where several machines on a single factory floor transmit data to central node or server. These several nodes or server then transmits the data to cloud where node.js server is implemented to store and manipulate the data. This data can be fetched by JOT officials and authorized clients by using RESTful API's and micro-services. End user, who might be a service engineer, JOT client or JOT R&D authorized employee can visualize the data anytime by send request to designated URL. In present case, visualization can be retrieved by send request to following URL using any web-browser.

URL: <https://ec2-34-224-218-137.compute-1.amazonaws.com:3443/#/>

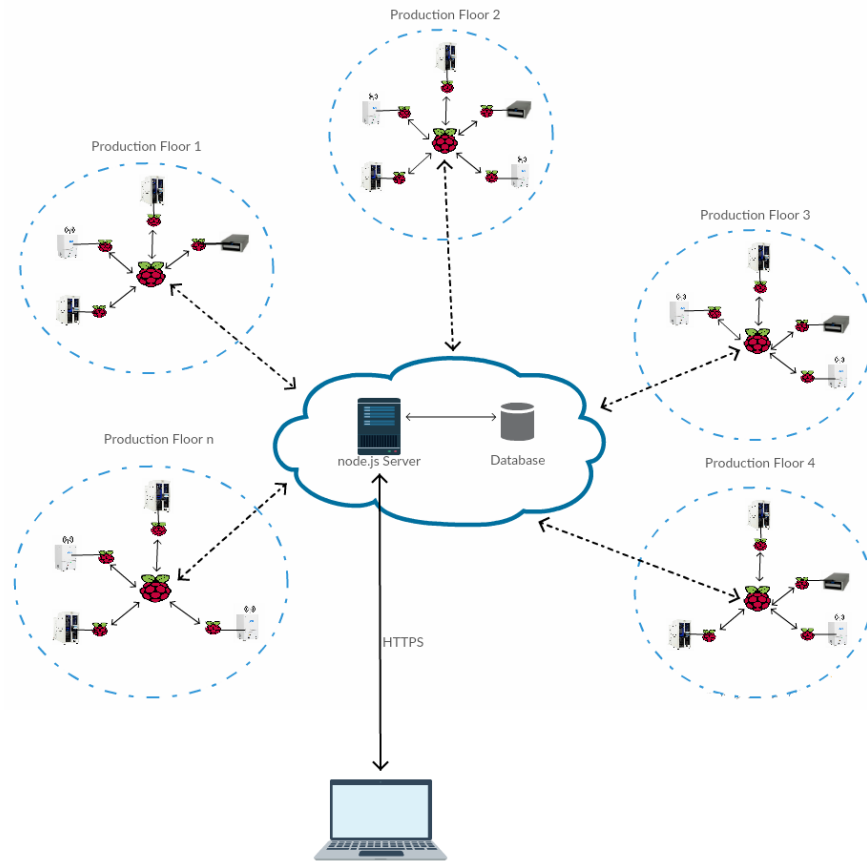


Figure 4.8: Star of stars topology for whole system

4.5 Advantages

There are number of advantages of using concept of IIoT on factory floor few of them are, receiving continuous feedback from systems, based on those feedbacks find the failure points of any system or machine, improve efficiency of machine, provide online support to customers which will add a feature and eventually help in generating revenue.

To take more benefits, this research needs to be carried forward to design a generic framework for plug and play solution. Moreover, there need to be have a drag and drop user design which will allow the end user to design dashboard according to its own needs. Implementations of some sort of algorithms on incoming data will also help the end user in forecasting and prediction. In addition to this, IIoT can also be used to keep tracks of goods on factory floor.

5. CONCLUSIONS

Fourth industrial revolution is happening right now and influence of internet connected technologies not just adds the value for organizations but also opens new business areas and opportunity of employment. There is need to rethink what is desired output organization needs from this revolution. Provided solutions are based on previous studies and industrial standards. According to world economic forum, industries ranging from manufacturing to transportation, healthcare and agriculture is using this technology and taking most out of it. Some of the manufacturing industries who are using this technology seriously are Bosch, Schneider Electric, General Electric and Siemens.

This thesis presents the optimize and distributed approach to concept of Industrial Internet of Things with different scenarios to open the new business domains to small and medium size organizations by explaining the practical implementation of problem faced by JOT Automation. Proposed system performs independently and can be connected with any industrial equipment with modification in construction of payload. The provided architectural solutions are robust. During this research work main task was to provide distributed, bi-direction, secure and efficient solution regardless the state of machine which was achieved by using MQTT, HTTP hybrid communication protocols with MEAN stack. The selection of hardware and cloud support was merely based on problem and cost.

Security risk of information was the major concern while implementation, which was minimized by studying and selecting appropriate technology. Data encryption was achieved by using SSL certificates and TLS. In addition to that, this research work also provides the detailed overview of IIoT stack and communication protocols, which can be used to introduce new architectural approach.

6. REFERENCES

- [1] D. U. H. Michahelles, "An Architectural Approach Towards the Future Internet of Things," 2011.
- [2] vulnerable, "Industry 4.0," *Interface*, no. Electrochemical Society, p. 4, 2014.
- [3] J. W. Abbott, "Applied predictive analytics: Principles and techniques for the professional data analyst," 2014.
- [4] V. Roblek, "A Complex View of Industry 4.0," *SAGE*, p. 11, 2016.
- [5] T. M. B. & B. J. Šalamon, "Late payments and ethics of management: Possible solutions for local economies," *Lex Localis—Journal of Local Self-Government*, p. 400, 2015.
- [6] H. P. James Haight, "IoT Analytics in Practice," *Analyst Insight*, p. 12, 2015.
- [7] A. Jamwal, "The Industrial Internet: Six Ways Manufacturers Can Fuse Big Data, Automation and IoT for Better Operations," *IoT and the Digitization of Manufacturing*, p. 6, 2016.
- [8] S. Zurier, "IIoT companies prove value of internet-connected manufacturing," *TechTarget | IoT Agenda*, p. 6, 2016.
- [9] B. Butler, "Most powerful Internet of Things companies," *Network World*, p. 2016, 10.
- [10] P. Tracy, "Top 5 industrial IoT companies," *rcwireless*, p. 8, 2016.
- [11] D. M. et, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, pp. 1497-1516, 2012.
- [12] J. L. Hill, "System Architecture for Wireless Sensor Networks," University of California, Berkley, 2003.
- [13] B. Horan, "Practical Raspberry Pi," 2013.

- [14] B. Stern, "Getting Started with FLORA," *adafruit*, 2015.
- [15] J. Yoshida, "IoT Processor List," *EE Times*, p. 4, 2016.
- [16] T. Lee, "The Hardware Enablers for the Internet of Things," *IEEI | Internet of Things*, 2015.
- [17] G. SCHATZ, "Mesh Network Topology: Pros and Cons For M2M Communication," *LinkLabs*, p. 6, 2016.
- [18] L. Frenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee," *Electronic Design*, p. 8, 2013.
- [19] B. RAY, "ZigBee Vs. Bluetooth: A Use Case With Range Calculations," *LinkLabs*, p. 10, 2015.
- [20] B. RAY, "5 Types of Wireless Technology For The IoT," *Link Labs*, 2015.
- [21] C. H. Kuor, "Bluetooth : A Viable Solution for IoT?," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 6-7, 2011.
- [22] J. H. Christophher, "Internetworking with Bluetooth Low Energy," *Mobile Computing and Communications*, pp. 34-38, 2015.
- [23] C. J. Hansen, "Internetworking with Bluetooth Low Energy," *Mobile Computing and Communications*, vol. 19, no. 2, pp. 34-38, 2015.
- [24] C. J. Hansen, "Internetworking with Bluetooth Low Energy," vol. 19, no. 2, pp. 34-38, 2015.
- [25] Q. M. Z. S. C. H. Jun, "Energy-efficient MAC Protocol Designed for Wireless Sensor Network for IoT," *Seventh International Conference on Computational Intelligence and Security (CIS)*, 2011.
- [26] "New Weightless 2-Way Communication IoT Standard launches".
- [27] A. B. A. Rahman, "Comparison of Internet of Things (IoT) Data," vol. 2, p. 21, 2015.
- [28] v. Patel, "WLAN," Gujarat, 2016.
- [29] T. Lammle, "Wireless LANs Advantages and Disadvantages," 2011.

- [30] G. B. a. A. P. D. Baldo, "The Siesta Project : Near Field Communication," pp. 721-725, 2010.
- [31] K. O. V. Coskun, Near Field Communicatioin (NFC), 2012.
- [32] P. Viswanathan, "Near Field Communication: Pros and Cons," Life Wire, 2014.
- [33] C. V. Ozdenizci B., "NFC Internal: An Indoor Navigation System," 2015.
- [34] O. Kaven, "Understanding Z-Wave Networks, Nodes & Devices," 2015.
- [35] "Understanding Z-Wave Networks, Nodes & Devices," 2015.
- [36] R. C. R. L. a. J. S. P. Amaro, "Implementing an Advanced," *International Youth Conference on Energetics*, 2011.
- [37] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," CISCO White Paper, 2011.
- [38] P. Ganguly, "Selecting the right IoT Cloud Platform," in *International Conference on Internet of Things and Applications (IOTA)*, Nagpur, India, 2016.
- [39] A. Z. Paolo Bellavista, "Towards Better Scalability for IoT-Cloud Interactions," *IEEE*, p. 6, 2016.
- [40] K. Holm, "Using MQTT Protocol Advantages," IBM developerWorks, 2012.
- [41] P. Patierno, "Comparison between some of the most importat Internet of Things and M2M," 2014.
- [42] M. Kowalke, "The Pros and Cons of the Major IoT Communications Protocols," 2015.
- [43] M. K. N. Ajit A. Chavana, "Secure and Cost-effective Application Layer Protocol with," Science Direct, Nagpur, 2015.
- [44] K. H. C. B. Z. Shelby, "The Constrained Application Protocol," 2014.
- [45] M. K. N. Ajit A. Chavana, "Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT," ScienceDirect, Nagpur, 2015.
- [46] J. G. N. C. L. Rodrigues, "RELOAD/CoAP Architecturewith Resource

Aggregation/Disaggregation Service," 2016.

- [47] M. Jones, "Meet the Extensible Messaging and Presence Protocol (XMPP)," 2009.
- [48] Charles Gibbons, "Internet of Things, M2M, Protocols, Actuators, Sensors, XMPP, HTTP, MQPP, MQPP," 2014.
- [49] Jesse, "The advantages and disadvantages of XMPP," Online: Programer, 2014.
- [50] R. F. F. T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.0," RFC Editors, 1996.
- [51] R. Fielding, "Hypertext Transfer Protocol -- HTTP/1.1," Compaq/W3C, 1999.
- [52] S. B. Cooper, "The Advantages of Hypertext Transfer Protocol".
- [53] B. Moyer, "All about messaging protocols," *Electronic Engineering*, p. 10, 2015.